www.pwc.dk

INSPIRATION TIL SUCCES:
- BRANCHEVENT FOR DETAILBRANCHEN – SÅDAN SIKRE DU DIN NETBUTIK

Oktober 2016

pwc

Jørgen Sørensen

Partner, PwC Denmark's Consulting group – Security & Technology

M: +45 24945254
E: jgs@pwc.dk

Baggrund og erfaring

Jørgen er ansvarlig for vores konsulentydelser inden for cyber & informationssikkerhed samt privacy – Digital trust

Jørgens speciale er re-organisering og transformering af sikkerhedsfunktioner. I den forbindelse har han været in-sourced som sikkerhedschef hos bl.a. 3F, Danske Spil og Københavns Lufthavne.

Jørgen har flere års praktisk erfaring med etablering og rådgivning i relation til it-strategi, organisering, effektivisering og optimering samt etablering af sikkerhedsstyring og -processer. Han har ligeledes været ansvarlig for tekniske opgaver i relation til sikkerhedsopsætning og test af infrastruktur og cyber beredskab samt Incident Respond og cyber simuleringsøvelser.

Uddannelse

BSc Computer Science , Aalborg Universitet (1997)

CISM, CISSP, CISA, CGEIT. CRISK

References eksempler

3F (10 år)

Fungerende sikkerhedschef i 10 år med reference til Daglig Ledelse og sikkerhedsudvalget. Etablering og drift af sikkerhedsfunktionen, implementering af ISO27001, cyber beredskab, krisestyring og cyber Incident Respond. 2012 forestod kan forsvaret imod det 10 dage lange hacker angreb og den forensic undersøgelse der ledes frem til anholdelse hackerne

Danske Spil (2,5 år)

Fungerende sikkerhedschef i 2.5 med reference til sikkerhedsudvalget. Ansvarlig for implementering af ISO27001 og den efterfølgende certificering. Etablering af Cyber beredskab og Incident Respond samt processer for risikostyring og hvidvask

Københavns Lufthavne (5 år)

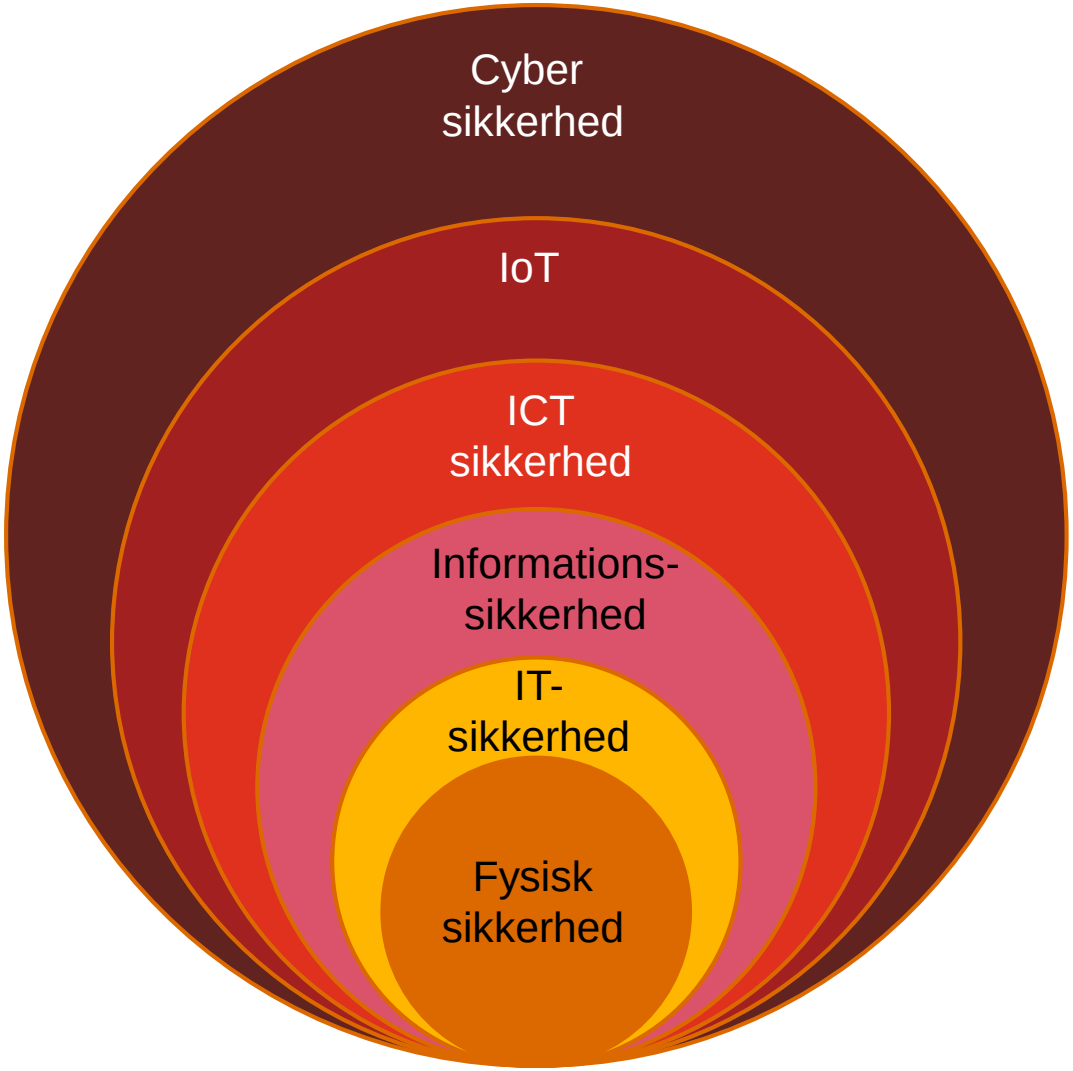
Fungerende sikkerhedschef i 5 år med reference til direktionen og sikkerhedsudvalget. Etablering og drift af sikkerhedsfunktionen, implementering af ISO27001, cyber beredskab, krisestyring og cyber Incident Respond. Test af særligt udstyr (Internet of Thing)

Hvad er cybersikkerhed?

- Cybersikkerhed kan betyde mange forskellige ting, afhængigt af hvem man spørger.
- Kendetegn og særlige egenskaber:
  - ***Bredere*** end bare informationsteknologi (it) og vedrører **ikke kun** organisationen.
  - ***Større sårbarhed*** som resultat af teknologisk konnektivitet og indbyrdes afhængighed.
  - Et "udefra-og-ind-perspektiv" på de ***trusler***, som organisationerne p.t. står over for, samt på ***indvirkningen på forretningen***.
  - Fælles ansvar, som kræver tiltag på tværs af funktionerne med henblik på at planlægge, beskytte, forsvare og reagere.

Ikke længere blot en it-udfordring – men en nødvendighed for hele forretningen!

Hvad er Cyber sikkerhed kontra informationssikkerhed



Pas på: Mere end 250 danske websider spreder ransomware

Forklaringen på den sidste tid mange ransomware-angreb er fundet. Massevis af danske websider er inficeret og spreder derfor ransomware, når en bruger besøger siden.

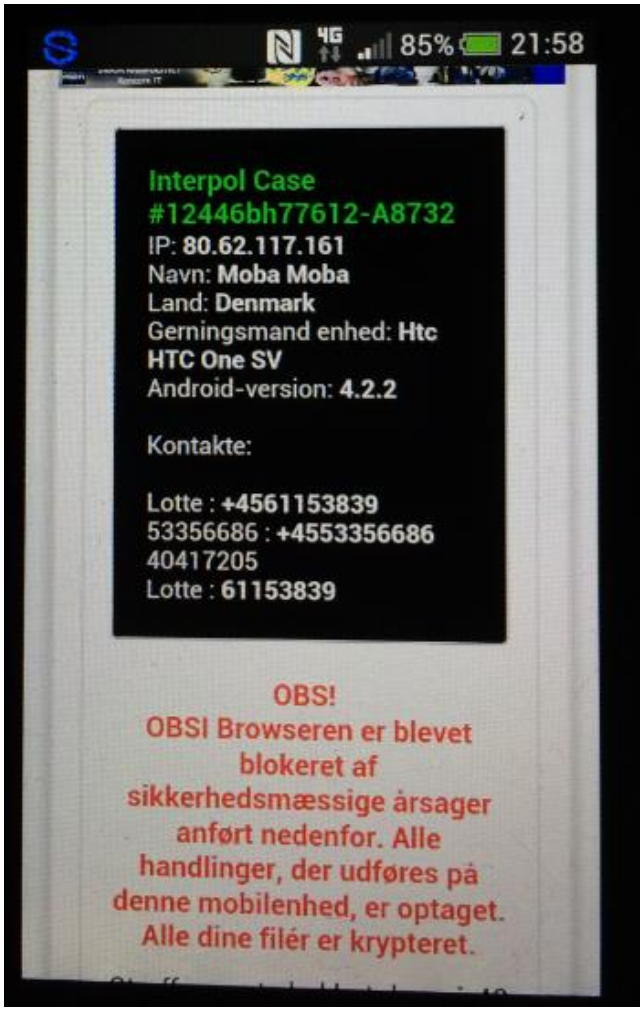
24. juli 2015 kl. 11.33

11 kommentarer

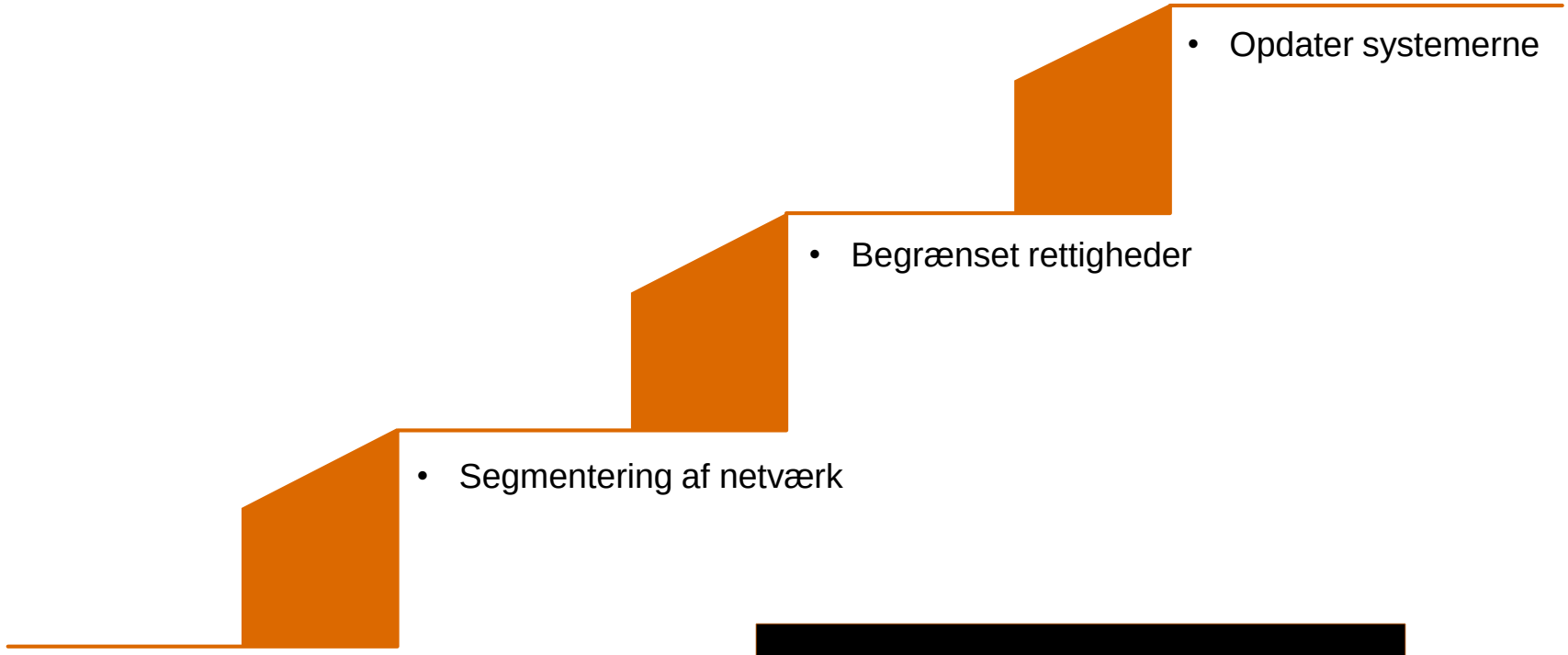
NICOLAI DEVANTIER
Journalist

Mange danske kommuner og virksomheder er i de senere måneder blevet ramt af ransomware.

Ransomware på mobil telefon



4 step der mindsker effekten af Ransomware

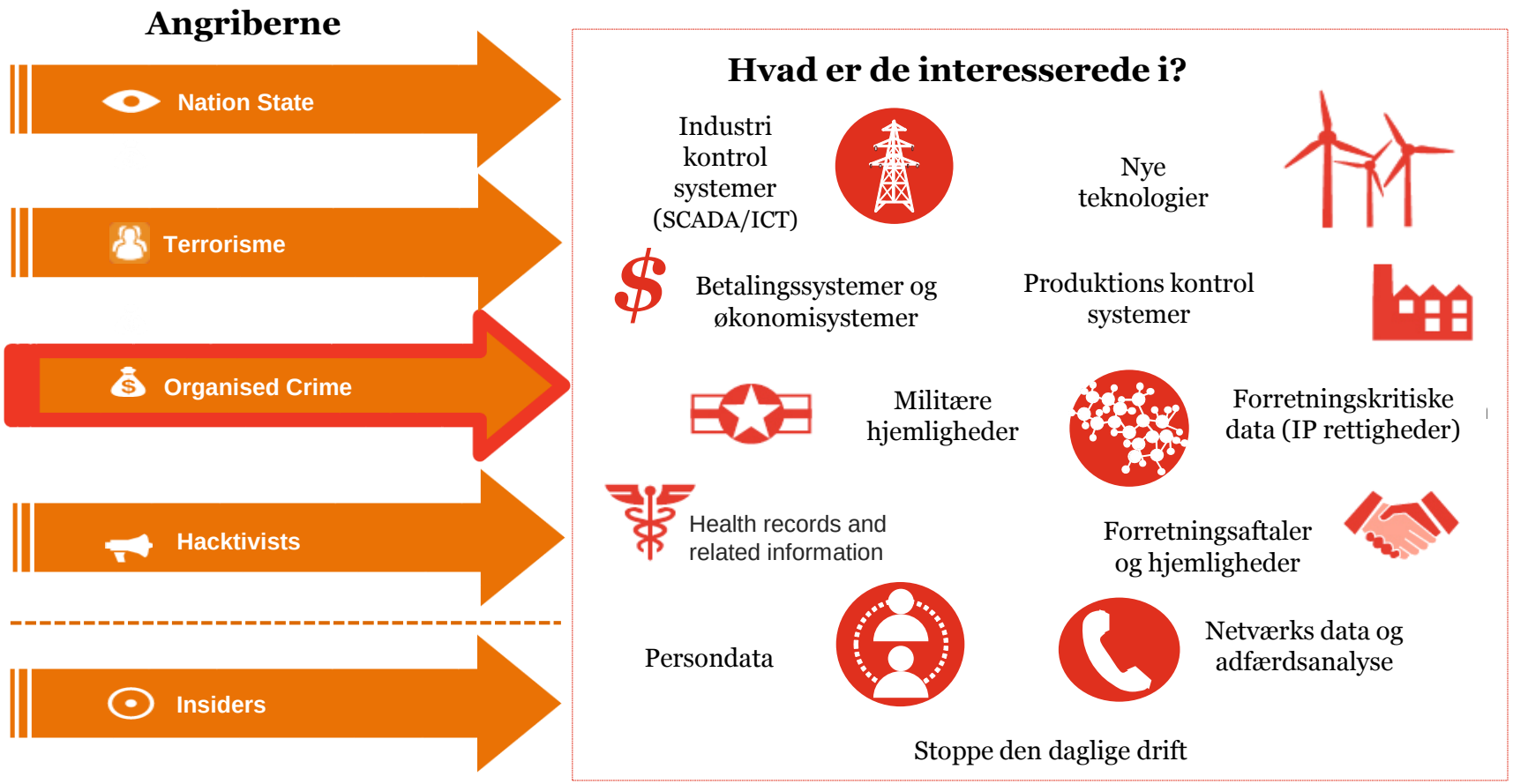


Men hvad med næste generation af malware

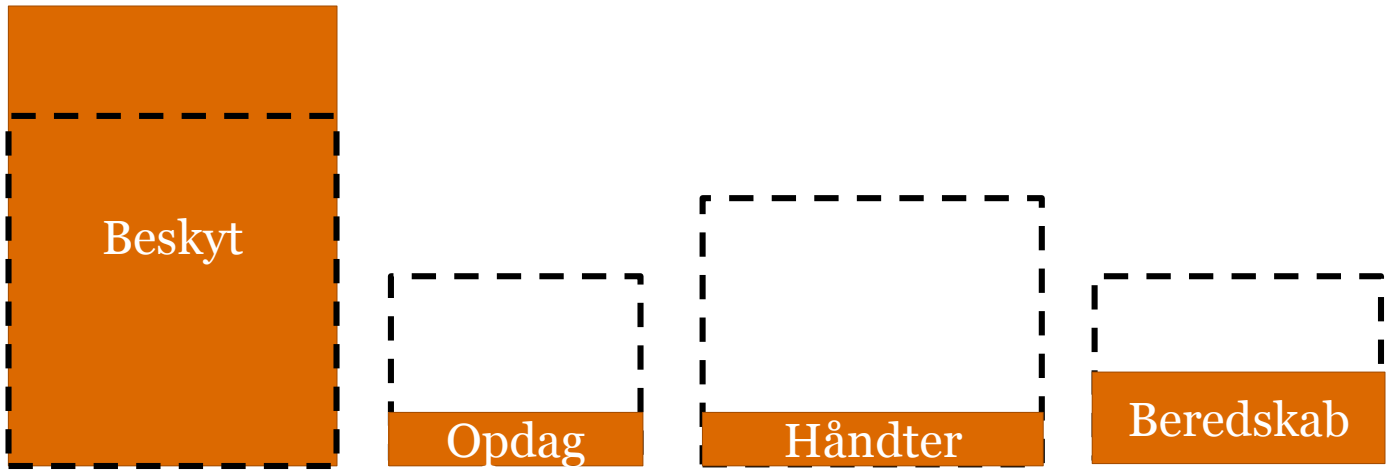
CEO fraud


Danske Bank
Privat
Erhverv
Private Banking
Søg
CEO Fraud step for step:
1. En Cyber kriminelle sender en mail til en medarbejder i bogholderiet.
2. Mailen ser ud til at komme fra virksomhedens topledere, der beordre medarbejderen om at lave en overførsler til en bank i udlandet.
3. Den cyber kriminelle følger op på mailen ved at ringe til personen der har fået mailen. Den kriminelle kan lyde meget troværdig og presser medarbejderen med historier om deadlines og store ordre
4. Når overførslen er foretaget, så flytter de cyber kriminelle beløbene til konti i andre banker
Derfor er det meget vigtigt, at jeres sikkerhedsprocedurer er i orden, og at medarbejdere er opmærksomme, når de modtager mistænkelige mails om overførsler til lande uden for Europa.

Angriberne og hvad de er interesserede i



Virksomhedens fordeling af sikkerhedsressourcer



Mange virksomheder har fokus på beskyttelse af deres systemer, data og infrastruktur.

Med de nuværende cyber trusler er det ikke en hensigtsmæssig prioritering

Virksomheder bør øge deres evne til at opdage, håndtere og reetablere efter et cyber angreb

Øget lovkrav

Ny EU persondataforordning

- Muligheder og risici ved digitaliseringen

Bøderne

Bødeårsag	Offentlig	Privat
Brud på krav vedr. artikel: 23. Privacy by Design & Default 24. Delt ansvar 25. Begrænsninger for dataansvarlig uden for EU 26. Databehandler 27. Behandling under ansvar fra dataansvarlig/-behandler 28. Logning af aktiviteter 29. Samarbejde med myndigheden 30. Sikkerhed i behandlingen 31. Notifikation til myndighed 32. Notifikation til borger/kundeDat 33. Data Protection Impact Assessment (PIA) 34. Konsultation med myndighed ved High Risk	*10.000.000€/ ?*	Op til 10.000.000€ eller 2% af global omsætning afhængig af hvilket beløb der er størst
Brud på krav vedr. artikel: • Basis principper incl. Samtykke artikel 5,6,7 & 9 • Den registredes rettighed jf. artikel 12-20 • Non-compliance med et krav om midlertidig eller begrænset databehandling fra tilsynsmyndighed jf. artikel 53 (1b) • Overførsel ad persondata til modtager i et tredje land	*20.000.000€ / ?*	Op til 20.000.000€ eller 4% af global omsætning afhængig af hvilket beløb der er størst
Brud på krav vedr. artikel: • Non-compliance med et direkte krav fra tilsynsmyndighed jf.artikel 53 (!b)	*20.000.000€ ?*	Op til 20.000.000€ eller 4% af global omsætning

PwC – kan hjælp jer

Vi er med jer hele vejen

Vi hjælper

FØR

(Cyber risiko
Cyber sikkerheds test
CISO-services
Awareness)

Gode penge

Vi hjælper

UNDER

(Incident respond
Crisis Management)

Panik penge

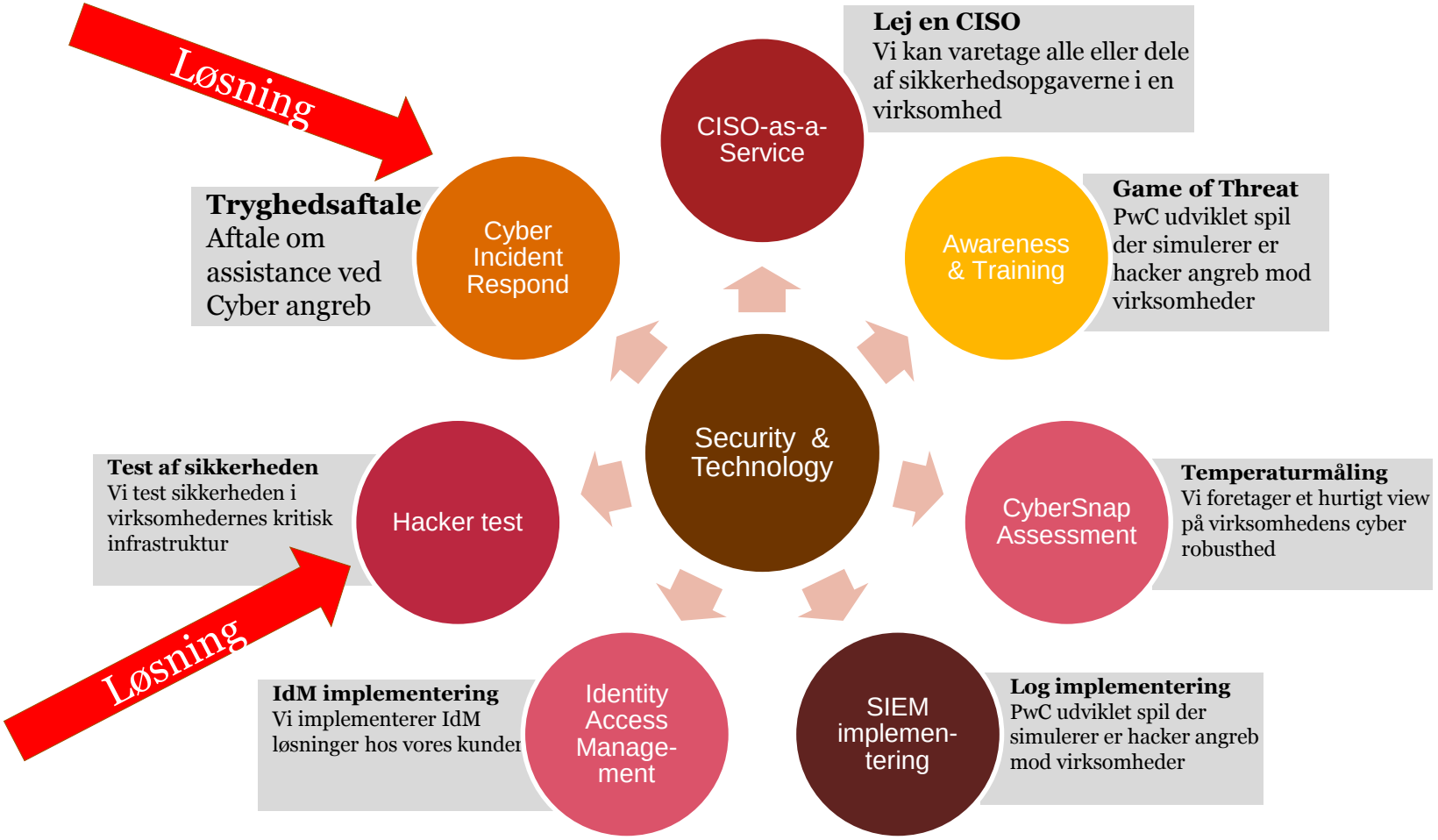
Vi hjælper

EFTER

(Cyber BCM
eForensic
Malware analyse)

Frustrations penge

Security & Technology – Services to our clients



4 hurtige tiltag